AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Twenty-seven (27) Google accounts, as further described in Attachment A

Case No. MJ17-275

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Twenty-seven (27) Google accounts, as further described in Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, which is attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, U.S.C. §1028A, 1029 Title 18, U.S.C. § 1030,1343 Title 18, U.S.C. § 1349, 371	Aggravated Identity Theft; Access Device Fraud; Computer Fraud; Wire Fraud; Conspiracy to Commit Wire Fraud; Conspiracy

The application is based on these facts:

See attached Affidavit of FBI Special Agent Armando Ramirez III

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

FBI Special Agent Armando Ramirez III
Printed name and title

Sworn to before me and signed in my presence.

Date: June 30, 2017

Judge's signature

City and state: Seattle, Washington

Mary Alice Theiler, U.S. MAGISTRATE JUDGE
Printed name and title

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, Armando Ramirez III, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. ***Agent Background:*** I am a Special Agent of the Federal Bureau of Investigation (FBI) currently assigned to the Seattle Field Division and have been employed as a Special Agent of the FBI since May 2006. I have received basic federal law enforcement training, including the training at the FBI Academy, as well as other specialized federal law enforcement training. In the course of my official duties as a Special Agent I have investigated a broad range of white collar crimes, including those involving copyright infringement, theft of trade secrets, bank fraud, wire fraud, mail fraud, health care fraud and money laundering. As a result, I have experience with the various methods and practices used by criminals to commit crimes through the use of computers, other digital devices, and the internet.

2. ***Email Accounts to be Searched:*** I submit this affidavit in support of an application for a search warrant pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A). The requested warrant would require Google, Inc., an internet service provider located at 1600 Amphitheater Parkway, Mountain View, California 94043, to disclose to the government copies of the information contained in the Google accounts discussed below. The warrant would authorize the search of email accounts operated by two individuals. These individuals are believed to be trafficking in stolen credentials that allow a user to obtain unauthorized access to proprietary digital databases such as those maintained by providers of digital content such as Getty Images, Inc.

3. The first set of email accounts are believed to be controlled by an individual who uses the online nickname "Milosevic." The Milosevic accounts are listed below as items a through u:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

a. im244562@gmail.com;
b. im514238@gmail.com;
c. 244562im@gmail.com;
d. blekpendaz@gmail.com;
e. carpetcleanerexpert8@gmail.com;
f. celebrityfascination@gmail.com;
g. hexenbiest316@gmail.com;
h. hqphotosworld@gmail.com;
i. im250372@gmail.com;
j. im308009@gmail.com;
k. imilosevic514@gmail.com;
l. ivanka.b.milosevic@gmail.com;
m. jovna.milosevic@gmail.com;
n. joximilosevic@gmail.com;
o. Jump2times@gmail.com;
p. Jump6times@gmail.com;
d. lazypandamail@gmail.com;
r. m.jovana.joka98@gmail.com;
s. madonna.picture.sell@gmail.com;
t. Mmaria244562@gmail.com; and
u. nameless244562@gmail.com.

4. The second set of email accounts are believed to be controlled by an individual who uses the online nickname "Frhtlayout." The Frhtlayout accounts are listed below as items v through aa:

v. frhtlayout@gmail.com;
w. myfavouritenightmare@gmail.com;
x. daichi.bloodlust@gmail.com;
y. dmngsp@gmail.com;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

z. izildaddomingues@gmail.com; and

aa. paloma.discola@usp.br

5. These accounts, and the information to be provided for each account, are listed in Attachment A to this Affidavit. Upon receipt of this information, government-authorized persons will review that information to locate and seize the items described in Attachment B to this Affidavit.

6. ***Scope of Affidavit:*** The facts set forth in this Affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation including other law enforcement officers, review of documents and records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation, but rather those relevant to the question of whether probable cause exists to issue the requested search warrant.

7. Based on my training and experience and the facts set forth in this Affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 1029 (Access Device Fraud), 1030(a)(4) (Computer Fraud), 1343 (Wire Fraud), 1028A (Aggravated Identity Theft), 1349 (Conspiracy to Commit Wire Fraud), and 371 (Conspiracy) have been committed by persons controlling the above accounts, and further, that the accounts contain evidence of these crimes and of the identities of the perpetrators.

II. SUMMARY OF THE AFFIDAVIT

8. This investigation arose out of a criminal referral by Getty Images, Inc. ("Getty"). Getty is a Seattle-based company that licenses copyrighted images to customers in return for a fee. Getty maintains its images in a proprietary database that customers access using credentials issued to them by Getty. In 2016, in connection with a civil copyright lawsuit, Getty learned of an online forum called "After EF." Criminals use After EF to

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

communicate about the unlawful purchase and sale of credentials that allow users to access digital content, such as Getty's proprietary database, without paying the required licensing fee. One of the major sellers of unauthorized credentials on After EF is a vendor who uses the nickname "Milosevic." A witness who has agreed to cooperate with Getty and the government ("Witness 1") has informed the government that Witness 1 purchased Getty credentials from Milosevic over the internet on numerous occasions.

9. Milosevic used two Gmail accounts to communicate with Witness 1. The addresses for these accounts are im514238@gmail.com and im244562@gmail.com. In addition, Milosevic directed Witness 1 to pay Milosevic for credentials via a PayPal account. According to PayPal records, the emails associated with the PayPal account are im514238@gmail.com and im244562@gmail.com.

10. The government applied for and obtained an order pursuant to 18 U.S.C.§ 2703(d) directing Google to disclose subscriber information for im514238@gmail.com and im244562@gmail.com (hereafter, the "Original Milosevic Accounts"). Information provided by Getty, Witness 1, Google, and other evidence, establishes probable cause to believe that the Original Milosevic Accounts contain evidence of trafficking in stolen user credentials and evidence of Milosevic's true identity.

11. The 2703(d) Order also required Google to produce subscriber information for accounts that are linked with, that is, that share common subscriber information with, the Original Milosevic Accounts. The material produced by Google, along with other evidence discussed below, establishes probable cause to believe that the accounts identified in paragraphs 3c through 3u above (hereafter the "Linked Milosevic Accounts") are operated by the same user that operates the Original Milosevic Accounts. Based on my training and experience, I know that email accounts typically contain evidence of the identity of the person operating the account. Therefore, there is probable cause to believe that the Linked Milosevic Accounts contain evidence of Milosevic's true identity, as well as evidence of Milosevic's unlawful trade in digital credentials.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

12. Another trafficker active on the AfterEF forum uses the nickname "Frhtlayout" and communicates with purchasers using the Gmail account frhtlayout@gmail.com. There is probable cause to believe that this account (hereafter the "Original Frhtlayout Account") contains evidence of trafficking in stolen credentials and of the identity of the person doing so. The Court's 2703(d) Order also required Google to produce subscriber information for accounts linked with the Original Frhtlayout Account. Google's response to the 2703(d) Order, along with other evidence, establishes probable cause to believe that the accounts identified above as items v through aa (the "Linked Frhtlayout Accounts") are operated by the same person that operates the Original Frhtlayout Account, and therefore are likely to contain evidence of Frhtlayout's true identity, as well as evidence of Frhtlayout's unlawful trade in digital credentials.

III. THE INVESTIGATION

A. The Getty Images Referral

13. In early March 2017 the United States Attorney's Office ("USAO") was contacted by an attorney representing Getty Images, Inc., a Seattle-based company that licenses copyrighted digital images. Getty's attorney reported that Getty was aware of a criminal network of individuals that trades in stolen credentials that allow users to unlawfully access digital content proprietary to Getty and other companies that license digital content. According to Getty's attorney, the network communicates over an online members-only forum known as "AfterEF."

14. On April 6, 2017, representatives of the USAO and Homeland Security Investigations met with Getty representatives, who provided information and evidence relating to the reported criminal activity. The Getty representatives explained that Getty maintains an online database containing millions of copyrighted images. The database is hosted on a server in King County, Washington. Getty's website offers users the ability to obtain copies of the images by paying a license fee and entering into a license agreement with Getty.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

15. Many of Getty's customers are large institutions such as newspaper companies or internet news sites. Getty issues credentials to these companies that allow the customers to download and view large numbers of images from Getty's database. The customers are not charged for downloading the images. Rather, under agreements between Getty and the customers, the customers periodically report to Getty which images the customer has used in its publications. Getty then invoices the customers for the value of these images. Under this system, an unauthorized third party who gains access to the credentials of a Getty customer may download thousands of images without the knowledge of Getty or the customer, thereby obtaining valuable images without paying the licensing fee. Getty is aware of hundreds of thousands of images that have been unlawfully downloaded in this manner.

B. The Civil Litigation and Discovery of AfterEF

16. On June 8, 2016, Getty filed a federal copyright infringement lawsuit against an Ohio resident named Walter Kowalczuk. *See* U.S. District Court for the Northern District of Ohio, Cause No. C16-1400. The lawsuit alleged that Kowalczuk had downloaded, without authorization, tens of thousands of images belonging to Getty, and subsequently offered those images for sale over the internet. Getty obtained a restraining order freezing Kowalczuk's assets, and ultimately obtained a judgment against him for $14,024,250.

17. Getty representatives informed the government that, in connection with the civil litigation, Kowalczuk disclosed that Kowalczuk had obtained the stolen images by accessing Getty's database with Getty customer credentials Kowalczuk had purchased from another person ("Witness 1"). Getty contacted Witness 1. Witness 1 admitted that Witness 1 had sold Getty credentials to Kowalczuk and others. Witness 1 ultimately entered into a settlement with Getty under which Witness 1 agreed to pay Getty a cash payment, and also to cooperate with Getty in its investigation into trafficking in Getty credentials.

18. Witness 1 told Getty representatives that Witness 1 had purchased Getty credentials over a members-only forum called "AfterEF." Witness 1 told Getty that he purchased credentials primarily from four vendors that he met through AfterEF. One of those vendors used the nickname "Milosevic," and is discussed further below. Witness 1

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

told Getty that, after purchasing the credentials, he usually used the credentials to access protected images, which he then sold to customers. Witness 1 said that he also sometimes resold the credentials.

19. Witness 1 told Getty that only members can access the AfterEF forum and must have AfterEF credentials to do so. A person can become an AfterEF member only if existing members of the forum vouch for him or her. By the time Witness 1 was contacted by Getty, Witness 1 was no longer selling stolen images and no longer held AfterEF credentials. At Getty's request, Witness 1 rejoined AfterEF and provided his AfterEF login credentials to Getty.

20. Using the credentials, Getty representatives logged on to the website. Getty captured screenshots and provided copies of some of the screenshots to the government. The screenshots show that there are approximately 70 members of the AfterEF forum. Each member is identified by a pseudonym, or nickname, and is assigned a rating of between one and five stars. In addition, some of the members are listed as a "trusted seller/buyer." Members create profiles, which allow the members to advertise what types of digital media credentials each member offers for sale. The website allows members to contact one another through private messaging or email by clicking a button next to the member's name.

21. In addition to private communications between members, AfterEF members engage in bulletin-board-style discussions about the purchase, sale, and use of credentials for media sites including Getty. These bulletin boards are open to all AfterEF members, but not to the general public. For example, one posting recommends that users wipe all metadata from downloaded pictures so that the source of the image cannot be traced. The posting also recommends that purchasers avoid using credentials on weekends, and warns that this will result in the account being "closed the following Monday."

C. "Milosevic" and the Original Milosevic Accounts

22. I conducted a telephonic interview of Witness 1 on June 26, 2017. Witness 1 confirmed the information described above that Witness 1 had previously provided to Getty. Witness 1 said that one of the AfterEF members who sold him credentials operates under the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

pseudonym "Milosevic" and uses the screen name "thatisnotmyname." Witness 1 believes that Milosevic is one of the largest sellers of credentials on AfterEF.

23. Printouts from the AfterEF forum confirm that a vendor using the screen name "thatisnotmyname" is a four-star "trusted seller/buyer" who has been a member of AfterEF since October 2013, and has posted approximately 878 posts. The profile page for "thatisnotmyname" contains a list of over 150 sites for which thatisnotmyname offers "HQ logins" (believed to mean high quality login credentials). The list includes Getty Images, as well as other providers of digital content such as AP Images, Fox Searchlight, HBO GO, and MGM Media Licensing. The vendor page also states that thatisnotmyname/Milosevic is located in Serbia.

24. Witness 1 stated that Witness 1 had communicated with Milosevic about purchasing Getty credentials over email on over 100 occasions. Milosevic used two email accounts for these communications: im514238@gmail.com and im244562@gmail.com. Witness 1 also provided Getty with PayPal records reflecting payments that Witness 1 made to Milosevic for digital credentials. The PayPal records list approximately 40 transactions between Witness 1 and a person with a U.K. verified PayPal account under the name "Daniel Knight." The email address associated with the PayPal account is listed as im244562@gmail.com for transactions occurring between September 2013 and October 2013, and as im514238@gmail.com for transactions occurring after November 2013.

D. Frhtlayout and the Original Frhtlayout Account

25. Another AfterEF member identified on the AfterEF screenshots provided by Getty uses the screen name "Frhtlayout." Frhtlayout is listed as a three-star trusted seller and buyer who has been a member of AfterEF since 2013, and who has made approximately 366 posts to the site. On at least 14 different postings, Frhtlayout invites interested buyers to contact him/her at the email address "frhtlayout@gmail.com."

26. The AfterEF screenshots provided by Getty include Frhtlayout's user profile. On the profile, Frhtlayout advertises that he/she is "selling logs" (presumably login credentials) and "pics" (images). The page contains a list of approximately 150 different

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

media organizations such as Getty, Sony Classic Pictures, and Home Box Office, and states that Frhtlayout is offering logins for these organizations, and that "there are more agencies available." Frhtlayout states that "all logs are untraded & have access to hi-res images." (An "untraded" login credential is a credential that has not been sold to another buyer, and which is therefore expected to remain valid for longer than a "traded" login credential.) The profile page goes on to advise prospective customers to "please, keep in mind I'm not responsible if it die fast. I'm always giving tips how to use it carefully, though. (Specially for fragile logs.)"

IV. THE 2703(D) ORDER AND RESPONSE: MILOSEVIC ACCOUNTS

A. The 2703(d) Order

27. Based on the foregoing evidence, on May 1, 2017, the government applied for an order directing Google to disclose subscriber information for im514238@gmail.com, im244562@gmail.com, (the "Original Milosevic Accounts") and frhtlayout@gmail.com (the "Original Frhtlayout Account") pursuant to 18 U.S.C. § 2703(d). The Order also directed Google to produce connection information, that is, records reflecting what other email accounts these accounts corresponded with. Finally, the Order directed Google to produce subscriber information for all Google accounts that are linked to the accounts listed in the Order either because they (1) share subscriber information (such as SMS phone number, recovery email address or creation IP address) with those accounts; or (2) Google has identified the accounts as "linked by cookies" because the accounts have been accessed by the same device. Google provided responsive information to the government on May 17, 2017.

B. Nature of Information Provided by Google

28. When an email user registers a Gmail account with Google, Google asks the subscriber to provide certain identifying information. The requested information includes, *inter alia*, the subscriber's name, a recovery email address, and a short messaging service ("SMS") number. In my training and experience, this information is valuable for establishing the account user's identity and for identifying and evaluating linked accounts,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

that is, accounts likely to be operated by the same user. Following is a description of categories of subscriber information relevant to this investigation.

29. ***User Name:*** Criminals using email accounts for unlawful purposes frequently use pseudonyms to register their accounts. Nonetheless, the user name provided to the email service can provide evidence significant in determining the user's identity. Often, a criminal will use the same pseudonym across multiple email accounts, which is evidence that the accounts may be operated by the same person. In addition, criminals sometimes use the same pseudonym to open an email account that they also use in communications on online criminal forums, which allows the investigator to draw connections between an email account and an online nickname.

30. ***Recovery Emails:*** Google asks subscribers to identify a "recovery email" that can be used to reactivate an account, reset a password, or otherwise communicate with the subscriber outside of the account itself. In my training and experience, subscribers generally list another authentic email account controlled by the subscriber as a recovery email address; otherwise the user risks losing access to the account. Recovery email addresses can therefore be used to identify other accounts controlled by the subscriber, which may contain evidence of the subscriber's identity. When two email accounts share a common recovery email account, this is generally a strong indication that the first two accounts are operated by the same person.

31. ***SMS Phone Number:*** Google also asks users to provide an SMS (short message service) number for use in managing the email account. Subscribers generally list an authentic SMS number for the same reason that they generally use an authentic recovery email, that is, because it is important to the user that he or she actually receive notification from Google about the email account. The fact that two email accounts share an SMS number is generally a strong indication that the two accounts are operated by the same person.

32. ***Number Sequences in Email Address:*** Sometimes the email address itself can provide evidence that two email accounts are controlled by the same user. For example,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

criminals, like other email users, sometimes use number sequences such as birthdates or other numbers of significance to them across different accounts. When an unusual number sequence is used in two different accounts, this commonality can be evidence that the accounts are controlled by the same user.

33. ***Accounts Linked By Cookies:*** Google uses a technology known as a "cookie" to track what particular devices (such as individual laptops, tablets, or smartphones) have been used to log into a Gmail account. When Google identifies two Gmail accounts as being linked by cookies, this means that the exact same device has been used to access both email accounts. Thus, if accounts are linked by cookies, this is a very strong indicator that the accounts are controlled by the same person or, at a minimum, people who share a device. It should be noted that, for various reasons, Google is not always able to track cookies; therefore the fact that two accounts are not linked by cookies does not suggest the accounts are not operated by the same person.

34. ***IP Login Information:*** Google typically retains records of the Internet Protocol ("IP") address used to register the account and, sometimes, the IP addresses associated with subsequent logins to the account. IP addresses can sometimes be used to identify the physical location of the user. The IP address associated with a particular location can change over time or can be "spoofed" or manipulated by the user, and therefore is not always reliable. However, use of a common IP by two different email accounts is evidence that the accounts may have been accessed from the same physical location or wireless network, and therefore potentially by the same person or related people.

C. Account Information Provided for Original Milosevic Accounts

1. im244562@gmail.com

35. As discussed above, Milosevic used the email account with the address "im244562@gmail.com" to communicate with Witness 1 about the purchase and sale of unauthorized Getty credentials. In addition, at Milosevic's instruction, Witness 1 paid for the unauthorized credentials by sending money to a PayPal account linked to this Gmail address.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

36. Google's response to the 2703(d) Order provided the following subscription information for this account:

Name: Ivancica Milosevic
Recovery Email: siera@sbb.rs
SMS: 38164574238
Associated IP Addresses: 178.149.197.6 and 188.2.137.162

37. Publicly-available records indicate that the domain associated with the email recovery email address (sbb.rs) is Serbia Broadband ("SBB"), Serbia's largest provider of telecommunications services. In addition, Google's response to the 2703(d) Order indicates that the SMS number 38164574238 is a Serbian number. According to an online IP lookup tool, both IP addresses that were used to access the im244562@gmail.com account are registered to SBB and assigned by SBB to SBB customers. These connections to Serbia are consistent with Milosevic's AfterEF profile page, which lists "Serbia" as Milosevic's location.

38. Google's response also identified three accounts as being "linked by cookies" with the im244562@gmail.com account. These are im514238@gmail.com (the other Original Milosevic Account), im250372@gmail.com, and lazypandamail@gmail.com. These accounts are discussed below under the heading "Linked Accounts."

39. Google's response also identified the email addresses for the accounts that the im244562@gmail.com account communicated with. Many of those accounts appear to be accounts managed by people in the business of buying and selling images over the internet. For example, the account contains many communications with the account frhtlayout@gmail.com. As discussed above, Frhtlayout is also an active vendor on the AfterEF forum. In addition, the connection records showed numerous communications between the account and Witness 1's Gmail account, which is mrphotoguy1@gmail.com. The im244562@gmail.com account also communicated with numerous other accounts whose names suggest that the user is involved in buying or selling images. These include worldphotographs@btinternet.com, mimoimages@gmail.com, fantasyartstudio@yandex.ru, star-gazer@mail.ru, and trocaphotos@hotmail.com. In addition, the im244562@gmail.com

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

account communicated with the account knightdj@btinternet.com. The PayPal account Milosevic used in selling images to Witness 1 is held in the name "Daniel Knight" and is identified by PayPal as a U.K. Verified Account. BT is a telecommunications provider that provides email and other services to United Kingdom residents.

2. im514238@gmail.com

40. As discussed above, Milosevic also used the email address im514238@gmail.com to communicate with Witness 1. Google's response to the 2703(d) Order provided the following subscription information for this account:

> Name: Ivanka Milosevic
> Recovery Email: siera@sbb.rs
> SMS: 38164574238
> Associated IP Addresses: 178.149.72.177 and 178.149.197.6

The recovery email, the SMS number, and one of the two IP addresses (178.149.197.6) is the same as the information associated with the im244562@gmail.com account (the other Original Milosevic Account). The other IP address, 178.149.72.177, is an address controlled by SBB and assigned to SBB customers.

41. Google also identified three accounts as being "linked by cookies" with the im514238@gmail.com account. These are the im244562@gmail.com account (the other Original Milosevic Account), im250372@gmail.com, and lazypandamail@gmail.com. The latter two accounts are the same two accounts linked by cookies with the im244562@gmail.com account.

42. As with the other Original Milosevic Account, Google provided connection information identifying the email accounts with which the im514238@gmail.com account communicated. These include many of the same parties that communicated with im244562@gmail.com, including many communications with frhtlayout@gmail.com and Witness 1. The account also contains numerous communications with sales@worldphotographs.com, poldergal-images@yahoo.com, and celebdise@gmail.com. Based on online web research, celebdise@gmail.com is the email address for a business called Celebrity Paradise, which advertises "image accounts" and "untraded logs" (login

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

information) for Getty and other providers of digital content. The account also contains many email communications with knightdj@btinternet, which may be connected with the "Daniel Knight" PayPal Account.

D. Account Information for Linked Milosevic Accounts

1. Overview of Evidence Relating to Linked Milosevic Accounts

43. ***Evidentiary Value of Linked Accounts:*** As discussed above, the 2703(d) Order directed Google to produce subscription information for accounts linked to the Original Milosevic Accounts, that is, accounts that contain common subscriber information with those accounts. Linked accounts can have substantial evidentiary value in computer crime investigations. Computer criminals often use certain email accounts ("dirty accounts") to conduct their criminal activities, and other accounts ("clean accounts") in their non-criminal activities. Both types of accounts provide important evidence. Dirty accounts provide evidence of the crimes under investigation. Of equal importance, clean accounts provide evidence of the user's true identity. When an investigator is able to link a dirty account with a clean account, this often allows the investigator to identify the criminal. Criminals do not always maintain a perfect separation between dirty and clean accounts, so each type of account may contain evidence both of criminal activity and user identity.

44. ***Summary of Linked Milosevic Account Information Provided by Google:*** Google produced subscriber information for 23 accounts linked to the Original Milosevic Accounts. This application seeks authority to search 19 of these accounts (the "Linked Milosevic Accounts"). The accounts are discussed individually below. All of the Linked Milosevic Accounts use the same recovery email address (siera@sbb.rs) and/or SMS number (38164574238), as the Original Milosevic Accounts. All of these accounts also share other commonalities with the Original Milosevic Accounts and one another. For example, the user name for many of the Linked Milosevic Accounts is "Ivanka Milosevic," or a variation of that name. Further, several of the Linked Milosevic Accounts contain the number sequences 244562 or 514328—the sequences used in the Original Milosevic Accounts—as part of the user name, email address, or recovery email address.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

45. In addition, many of the Linked Milosevic Accounts were accessed using the same IP addresses used to access the Original Milosevic Accounts, which tends to show that the respective Linked Milosevic Accounts were accessed from the same location as the Original Milosevic Accounts. In other cases, the Linked Milosevic Accounts were accessed by other IP addresses issued by the same telecommunications company (SBB) as the IP addresses used to access the Original Milosevic Accounts. SBB, like many telecommunications providers, controls ranges of IP addresses and assigns its users specific IP addresses within those ranges. For example, of relevance here, SBB controls the range or IP addresses from 178.149.0.0 through 178.149.255.255, as well as from 87.116.128.0 through 87.116.191.255. In my training and experience, it is common for a telecommunications company to change the IP addresses assigned to a certain customer over time. Therefore, the fact that the Linked Milosevic Accounts have been accessed by numerous different IP addresses controlled by SBB is consistent with the possibility of the same user accessing those accounts.

46. The relevant subscriber information for each Linked Milosevic Account is discussed below, and is summarized in a table attached as Appendix A to this Affidavit. The commonalities shown below between the Linked Milosevic Accounts and the Original Milosevic Accounts establish a high probability that each of the Linked Milosevic Accounts is controlled by Milosevic or, at a minimum, someone with a very close relationship to Milosevic. Therefore, there is probable cause to believe that the contents of these accounts will contain evidence of Milosevic's true identity, as well as additional evidence of Milosevic trafficking in unauthorized user credentials.

2. Subscriber Information for Specific Linked Milosevic Accounts

47. ***im250372@gmail.com:*** im250372@gmail.com is one of the accounts linked by cookies with (accessed using the same device as) both of the Original Milosevic Accounts. The user name for this account is "Ivanka Milosevic." The recovery email is im514238@gmail.com (one of the Original Milosevic Accounts), and the SMS number is 38164574238 (the same SMS number used for both Original Milosevic Accounts). This

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

account was accessed from IP 178.149.197.6, (the SBB-assigned IP address used to access both Original Milosevic Accounts), and IP 178.149.72.177 (the SBB-assigned address used to access im514238@gmail.com).

48. ***imilosevic514@gmail.com:*** The user name for this account is "Ivanka Milosevic." The recovery email is im514238@gmail.com (one of the Original Milosevic Accounts), and the SMS number is 38164574238 (the SMS number used for the Original Milosevic Accounts). In addition, the number sequence "514" in the account name is the first three digits of one of the Original Milosevic Accounts.

49. ***244562im@gmail.com:*** The user name for this account is "Ivanka Milosevic." The recovery email is siera@sbb.rs (the recovery email for both Original Milosevic Accounts), and the SMS number is 38164574238 (the number used for the both Original Milosevic Accounts). In addition, the number sequence "244562" in the account address is the same sequence used in the address of one of the Original Milosevic Accounts.

50. ***im308009@gmail.com:*** The user name for this account is "Ivanka Milosevic." The recovery email is im514238@gmail.com (one of the Original Milosevic Accounts); and the SMS number is 38164574238. In addition, this account was accessed using IP 178.149.197.6 (which was used to access both Original Milosevic Accounts), as well as 178.149.72.177 (which was used to access one of those accounts).

51. ***ivanka.b.milosevic@gmail.com:*** The user name for this account is "Ivanka Milosevic." The recovery email address is siera@sbb.rs, and the SMS number is 38164574238. In addition, the IP address used to access the account is 87.116.128.203, which is an SBB-assigned IP address.

52. ***Lazypandamail@gmail.com:*** As noted above, this account is linked by cookies with both of the Original Milosevic Accounts. The user name for the account is "lazy panda." The recovery email address for this account is siera@sbb.rs, and the SMS number is 38164574238. In addition, the IP address associated with the account is 178.149.197.6, which is the same IP address used to access both of the Original Milosevic Accounts.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

53. ***hqphotosworld@gmail.com:*** The user name for this account is "HQ Photos," which may stand for "high quality photos." The recovery email is siera@sbb.rs and the SMS number is 38164574238. In addition, the account was created using IP address 178.149.78.175, which is an SBB-assigned address that was also used to create the imilosevic514@gmail.com account described above.

54. ***Jump6times@gmail.com:*** The user name for this account is "Jump Tmes." The recovery email is Ivanka.b.Milosevic@gmail.com which, as discussed above, is closely linked to the Original Milosevic Accounts. The SMS number associated with this account is 38164574238. The account was accessed using an SBB-assigned IP address.

55. ***Jump2times@gmail.com:*** The user name for this account is "accountshq." The recovery email for this account is im244562@gmail.com (one of the Original Milosevic Accounts). The SMS number associated with this account is 38164574238. The account was created using an SBB-assigned IP address.

56. ***Carpetcleanerexpert8@gmail.com:*** The username for this account is "Marija Milivojevic." The recovery email for this account is im244562@gmail.com (one of the Original Milosevic Accounts), and the SMS number associated with this account is 38164574238. The account was created using an SBB-assigned IP address.

57. ***Joximilosevic@gmail.com:*** The user name for this account is "Joxi Milosevic." The recovery email account is siera@sbb.rs. There is no SMS number associated with this account. One of the IP addresses used to access the account is 178.149.72.177, which is one of the IP addresses used to access one of the Original Milosevic Accounts. The account was also accessed using another SBB-assigned IP address.

58. ***Jovna.milosevic@gmail.com:*** The user name for this account is "Jovna Milosevic." The recovery email account is siera@sbb.rs. There is no SMS number associated with this account. The account was accessed using an SBB-assigned IP address.

59. ***M.jovana.joka98@gmail.com:*** The user name for this account is "Jovana Milosevic." The recovery email is siera@sbb.rs. The IP address used to create the account

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

is 188.2.134.18, which is the same SBB-assigned IP address that was used to create the jovna.milosevic@gmail.com account.

60. ***Nameless244562@gmail.com:*** The user name for this account is "Nameless Nameless." The recovery email is siera@sbb.rs, and the SMS number associated with the account is 38164574238. The IP address used to open the account was 178.149.72.177, which was also used to open one of the Original Milosevic Accounts. In addition, the number sequence "244562" used in the email address is the same number sequence used in one of the Original Milosevic Accounts. This account was also accessed from the IP address 109.202.157.136. According to the Domain Tools whois lookup service, this IP address is assigned to a Danish telecom provider called Zen Systems. As discussed immediately below, this IP address was also used to access another Linked Milosevic Account at approximately the same time.

61. ***Hexenbiest316@gmail.com:*** The user name for this account is "Hexen Biest." There is no recovery email associated with the account, but the SMS number is 38164574238. In addition, the IP address used to open this account, 109.202.157.136 is the same address used to access the nameless244562@gmail account. According to the Google 2703(d) response, the nameless244562@gmail account and the hexenbiest316@gmail.com account were accessed from the 109.202.157.136 IP address within minutes of one another. The nameless244562@gmail.com account was accessed from this IP address at 11:33 UTC on April 3, 2017. The hexenbiest316@gmail.com account was accessed from the same IP address at 11:55 UTC on April 3, 2017.

62. ***Mmaria244562@gmail.com:*** The user name for this account is "Maria Magdelena." There is no recovery email associated with the account, but the SMS number is 38164574238. In addition, the number sequence 244562 used in the name of the account is the same sequence used in one of the Original Milosevic Accounts. The account was created using an SBB-assigned IP number.

63. ***Blekpendaz@gmail.com:*** The user name for this account is "Keka Nikolic." The recovery email is siera@sbb.rs. There is no SMS number for this account. However,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

the account was accessed from the IP address 178.149.72.177, which is the same IP address that was used to create one of the Original Milosevic Accounts. The account was also accessed from an IP number controlled by Serbia Telenor, another Serbian telecommunications provider.

64. ***Madonna.picture.sell@gmail.com:*** The user name for this account is "Siera Smith." The recovery email address is siera@sbb.rs, and the SMS number is 38164574238. The IP address, 188.2.141.193, is an SBB-assigned number.

65. ***Celebrityfascination@gmail.com:*** The user name for this account is "Lolo Admin." The recovery email is siera@sbb.rs, and the SMS number is 38164574238. The IP address, 178.149.64.213, is an SBB-assigned number.

66. Because each of these Linked Milosevic Accounts appears to be operated by Milosevic, there is probable cause to believe that the accounts will contain evidence of Milosevic's identity and of the criminal violations discussed above.

V. THE 2703(D) ORDER AND RESPONSE: FRHTLAYOUT ACCOUNTS

A. Account Information Provided for Original Frhtlayout Account

67. As discussed above, another active vendor on the AfterEF site uses the nickname "Frhtlayout." Frhtlayout's AfterEF postings invited buyers to contact him/her via the email address frhtlayout@gmail.com (the Original Frhtlayout Account). The 2703(d) Order requested subscriber information, linked accounts, and connection information for this account.

68. Google's response to the 2703(d) Order provided the following subscription information for this account:

> Name: P Domingues
> Recovery Email: myfavouritenightmare@gmail.com
> SMS: 5511998560016
> Associated IP Addresses: 177.81.142.224; 201.93.22.71; 189.46.62.229; 177.79.41.54; 177.102.115.248; 189.0.82.161; 191.254.165.252

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

69. Google's response indicates that the SMS number linked with the account is a Brazilian number. According to an online whois lookup service, all of the IP addresses are assigned to Brazilian telecommunications companies.

70. Google's response also identified two accounts as being "linked by cookies" with the frhtlayout@gmail.com account. These are myfavouritenightmare@gmail.com (which is also the recovery email for the Original Frhtlayout Account), and paloma.discola@usp.br. These accounts are discussed below under the heading "Linked Frhtlayout Accounts."

71. Google's response also identified the email addresses for the accounts that the frhtlayout@gmail.com account communicated with. Many of those accounts appear to be accounts managed by people in the business of buying and selling images over the internet. The connection records show that (consistent with the connection records for the Original Milosevic Accounts), the frhtlayout@gmail.com account corresponded extensively with both Original Milosevic Accounts. In addition, the Original Frhtlayout Account corresponded with numerous other accounts whose names suggest the account owner is engaged in the purchase or sale of images. For example, the corresponding accounts include photography.bkk@gmail.com, phototrades2012@gmail.com, photosasl@yahoo.com, ventes-photos@hotmail.fr, and drazphoto@gmail.com. Accordingly, there is probable cause to believe that this account will contain evidence of criminal violations and of the identity of Frhtlayout.

B. Subscriber Information for Linked Frhtlayout Accounts

72. ***Summary of Linked Account Information Provided by Google:*** Google also produced subscriber information for nine accounts linked to the Original Frhtlayout Account. This application seeks authority to search five of these accounts (the "Linked Frhtlayout Accounts"). All but one of the Linked Frhtlayout Accounts use the same recovery email address (myfavouritenighmare@gmail.com) and/or SMS number (5511998560016), as the Original Frhtlayout Account. All of these accounts also share other commonalities with the Original Frhtlayout Account and one another. For example, the user name for many of the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Linked Frhtlayout Accounts is "Paloma Domingues," or a variation of that name, which is consistent with "P Domingues," the user name for the Original Frhtlayout Account. Further, many of the Linked Frhtlayout Accounts were accessed using an IP address used by the Original Frhtlayout Account or another Linked Frhtlayout Account. Following is a discussion of each specific account. In addition, a chart summarizing the relevant subscriber information is attached as Appendix B to this Affidavit.

73. ***Myfavouritenightmare@gmail.com:*** The user name on this account is "Paloma Domingues," which is consistent with the name "P Domingues" on the Original Frhtlayout Account. This is the recovery email address for the Original Frhtlayout account and is one of the accounts that Google identified as linked by cookies with the Original Frhtlayout Account. This account also has the same SMS number (5511998560016) as the Original Frhtlayout Account. This email account was accessed from three of the same IP addresses that accessed the Original Frhtlayout Account.

74. ***Daichi.bloodlust@gmail.com:*** The user name for this account is "Daichi." The recovery email is myfavouritenightmare@gmail.com. The SMS number is 5511998560016. The account was created from a user at IP number 177.81.94.43, which is assigned to a Brazilian telecommunications provider.

75. ***dmngsp@gmail.com:*** The user name for this account is "Paloma Domingues." The recovery email is myfavouritenighmare@gmail.com. The SMS number is 5511998560016. The account was created using IP address 179.208.63.123, which is assigned to a Brazilian telecommunications provider.

76. ***izildaddomingues@gmail.com:*** The user name for this account is "Izilda Domingues." The recovery email is myfavouritenightmare@gmail.com. The SMS number is 5511998560016. The account was accessed from two different IP addresses that were also used to access the Original Frhtlayout Account.

77. ***paloma.discola@usp.br:*** The user name for this account is "Paloma Discola Domingues Silva." The account is linked by cookies with the Original Frhtlayout Account. In addition, the account was accessed from four IP addresses that were also used to access

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

the Original Frhtlayout Account. The recovery email associated with the account is paloma.discola@usp.br.test-google-a.com, and there is no SMS number for the account.[1]

VI. NATURE OF REQUESTED MATERIAL

A. Emails

78. In general, an e-mail that is sent to a Google subscriber is stored on Google servers until the subscriber deletes the e-mail. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to Google servers, and then transmitted to its end destination. Google often maintains a copy of received and sent e-mails. Unless the sender specifically deletes an e-mail from the Google server, the e-mail can remain on the system indefinitely. Even if the subscriber deletes the e-mail, it may continue to be available on Google's servers for some period of time.

79. A sent or received e-mail typically includes the content of the message, source and destination addresses, the date and time at which the e-mail was sent, and the size and length of the e-mail. If an e-mail user writes a draft message but does not send it, that message may also be saved by Google but may not include all of these categories of data.

B. Other Google Services

80. In addition to e-mail and chat, Google offers subscribers numerous other services including: Android, Blogger, Google Alerts, Google Calendar, Google Chrome Sync, Google Cloud Print, Google Developers Console, Google Drive, Google Hangouts, Google Maps, Google Payments, Google Photos, Google Search Console, Google Voice, Google+, Google Profile, Location History, Web & Activity, and YouTube, among others. Thus, a subscriber to a Google account can also store files, including address books, contact lists, calendar data, photographs and other files, on servers maintained and/or owned by Google. For example, Google Calendar is a calendar service that users may utilize to

---

[1] While the address for the account is not a "gmail.com" address, the subscriber information produced by Google indicates that Google controls at least some of the account information. The subscriber information states that the account uses Gmail and other Google services such as Google Groups and Google Drive. In addition, the fact that Google has provided subscriber information for the account and has determined that it is linked by cookies with the Known Frhtlayout Account demonstrates that Google has control of the account data.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

organize their schedule and share events with others. Google Drive may be used to store data and documents, including spreadsheets, written documents (such as Word or Word Perfect) and other documents that could be used to manage a website. Google Photos can be used to create photo albums, store photographs, and share photographs with others and "You Tube," allows users to view, store and share videos. Google Search Console records a Google account user's search queries. Google Web & Activity records certain browsing history depending on whether the account holder is logged into their account. Like many internet service companies, the services Google offers are constantly changing and evolving.

81. Based upon my training and experience, all of these types of information may be evidence of crimes under investigation. Stored e-mails and chats not only may contain communications relating to crimes, but also help identify the participants in those crimes. Address books and contact lists may help identify co-conspirators. Similarly, photographs and videos of co-conspirators may help identify their true identities, as opposed to supposed identities that they have used in telephone or e-mail communications. Documents (such as lists of IMEIs to be unlocked), may identify the scope of the criminal activity and calendar data may reveal the timing and extent of criminal activity.

C. Google Location History and Location Reporting

82. According to Google's website, "Location Reporting" allows Google to periodically store and use a device's most recent location data in connection with the Google Account connected to the device. "Location History" allows Google to store a history of location data from all devices where a user is logged into their Google Account and have enabled Location Reporting. According to Google "[w]hen you turn on Location Reporting for a device like your iPhone or iPad, it lets Google periodically store and use that device's most recent location data in connection with your Google Account." How often Location Reporting updates location data is not fixed. Frequency is determined by factors such as how much battery life the device has, if the device is moving, or how fast the device is moving. Google's location services may use GPS, Wi-Fi hotspots, and cellular network towers to determine an account holder's location.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

83. Based on the above, I know that if users of the target accounts utilize a mobile device to access the respective Gmail accounts identified in Attachment A-1 and have not disabled location services on their device/s or through the Google account settings, Google may have detailed records of the locations at which the account holders utilized the mobile device/s. This type of evidence may further assist in identifying the account holders, and lead to the discovery of other evidence of the crimes under investigation.

D. Customer Service Communications

84. In some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

VI. INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

85. Pursuant to Title 18, United States Code, Section 2703(g), this application and affidavit for a search warrant seeks authorization to permit Google, and its agents and employees, to assist agents in the execution of this warrant. Once issued, the search warrants will be presented to Google with direction to identify the accounts described in Attachment A to this Affidavit.

86. The search warrants will direct Google to create exact copies of the specified accounts and records.

87. The United States forswears the plain view doctrine in connection with any search for electronically stored evidence authorized by this warrant.

88. I, and/or other law enforcement personnel will thereafter review the copies of the accounts and records provided by Google, and identify from among that content those items that come within the list of items identified on Section II to Attachment B, for seizure.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

89. If the investigative team discovers any other content that may constitute attorney-client communications during their review of the filtered records for additional content that falls within the scope of the warrant, the investigative team will immediately cease their review of that particular item and segregate the item for further review by the filter team. The filter team shall not disclose the existence of or seize evidence or documents not covered by the warrant and shall not disclose any items that constitute attorney-client communications.

90. Analyzing the data contained in the accounts may require special technical skills, equipment, and software. It could also be very time-consuming. Searching by keywords, for example, can yield thousands of "hits," each of which must then be reviewed in context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. Keywords used originally need to be modified continuously, based on interim results. Certain file formats, moreover, do not lend themselves to keyword searches, as keywords, search text, and many common e-mail, database and spreadsheet applications do not store data as searchable text. The data may be saved, instead, in proprietary non-text format. And, as the volume of storage allotted by service providers increases, the time it takes to properly analyze recovered data increases, as well. Consistent with the foregoing, searching the recovered data for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques and may take weeks or even months. All forensic analysis of the data will employ only those search protocols and methodologies reasonably designed to identify and seize the items identified in Section II of Attachment B to the warrant.

91. Based on my experience and training, and the experience and training of other agents with whom I have communicated, it is necessary to review and seize a variety of e-mail communications, chat logs and documents, that identify any users of the subject accounts and e-mails sent or received in temporal proximity to incriminating e-mails that provide context to the incriminating communications.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

VIII. REQUEST FOR NONDISCLOSURE AND SEALING

92. The government requests, pursuant to the preclusion of notice provisions of Title 18, United States Code, Section 2705(b), that Google be ordered not to notify any person (including the subscriber or customer to which the materials relate) of the existence of these warrants for such period as the Court deems appropriate. In this case, such an order is appropriate because the search warrants relate to an ongoing criminal investigation and disclosure would provide the targets with information about the government's investigation that could be used to frustrate further investigative efforts.

93. The targets of this investigation have used a variety of anonymous web based e-mail accounts, cloud computing services, and other methods to obfuscate their identities while operating an online criminal enterprise. The targets of the investigation do not know the full extent of the government's knowledge of their communication channels and e-mail accounts. Much of the evidence in this investigation is electronically stored information. If alerted to the existence of the search warrants, the targets under investigation could destroy evidence, including information saved to their personal computers, information stored in other web based e-mail accounts or other online computing accounts. Additionally, if alerted to the existence of the search warrants, the targets could change patterns of behavior, notify confederates or take steps to avoid capture and prosecution. Accordingly, there is reason to believe that notification of the existence of the search warrants will seriously jeopardize the investigation or unduly delay a trial, including by giving targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, or intimidate potential witnesses. *See* 18 U.S.C. § 2705(b).

94. It is further respectfully requested that this Court issue an order sealing, all papers submitted in support of this application, including the application and search warrant. I believe that sealing is necessary for the same reasons stated above in support of my request for non-disclosure orders. I am requesting an extended sealing order of up to two years because some the targets of this investigation appears to be foreign nationals in counties from which it may be difficult to secure assistance or extradition. Should charges be filed,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

any efforts to identify and capture suspects who reside in Serbia or Brazil could take several years. For these reasons, I am requesting that the Court issue an order sealing the search warrant, search warrant return, application and affidavit for the search warrant, and all attachments, for up to two years, until charges are filed, or the investigation is closed, whichever event is earliest.

VIII. CONCLUSION

95. Based on the forgoing, I request that the Court issue the proposed search warrants. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that - has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Accordingly, by this Affidavit and Warrant I seek authority for the government to search all of the items specified in Section I, Attachments B (attached hereto and incorporated by reference herein) to the Warrant, and specifically to seize all of the data, documents and records that are identified in Section II to that same Attachment.

ARMANDO RAMIREZ III
Special Agent, FBI

SUBSCRIBED AND SWORN before me this 30 day of June, 2017

MARY ALICE THEILER
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Appendix A

Milosevic Email Account Summary

Address	Name	Recovery Email	IPs[i]	IP location	SMS	SMS Country	Cookies
Im244562 (Original Milosevic Account)	**Invancica Milosevic**	**siera@sbb.rs**	**188.2.137.162 178.149.197.6**	**SBB Modem SBB**	**38163574238**	**Serbia**	**IM514238 IM250372 lazypandamail**
Im514238 (Original Milosevic Account)	**Ivanka Milosevic**	**siera@sbb.rs**	**178.149.72.177 178.149.197.6**	**SBB SBB**	**38163574238**	**Serbia**	**Lazypandamail IM244562 IM250372**
244562im	Ivanka Milosevic	siera@sbb.rs	178.149.65.159		38163574238	Serbia	
blekpendaz	Keka Nikolic	siera@sbb.rs	217.65.199.82 178.149.72.177	Serbia-Telenor SBB			
Carpetcleanerexpert8	Marija Milivojevic	Im244562	178.149.71.129	SBB	38163574238	Serbia	
celebrityfascination	Lolo Admin	siera@sbb.rs	178.149.64.213	SBB	38163574238	Serbia	
G8wayphotos	Karen Bildebase	Karen@g8way.no	89.191.26.10	Norway	38163574238	Serbia	
Hexenbiest316	Hexen Biest		109.202.157.136	Norway	38163574238	Serbia	
hqphotosworld	Hq photos	Im514238	178.149.78.175	SBB	38163574238	Serbia	
Im250372	Ivanka Milosevic	Im514238	178.147.72.207 178.149.72.177 178.149.197.6	SBB SBB	38163574238	Serbia	
IM308009	Ivanka Milosevic	Im514238	178.149.65.17 178.149.72.177 178.149.197.6	SBB SBB SBB	38163574238	Serbia	
Imilosevic514	Ivanka Milosevic	Im514238	178.149.78.175	SBB	38163574238	Serbia	
Ivanka.b.Milosevic	Ivanka Milosevic	siera@sbb.rs	87.116.128.203	SBB	38163574238	Serbia	
Jovna.Milosevic	Jovna Milosevic	siera@sbb.rs	188.2.134.18	SBB Modem			
JoxiMilosevic	Joxi Milosevic	siera@sbb.rs	178.149.65.17 178.149.72.177	SBB		Serbia	
Jump2times	accountshq	IM244562	178.149.68.37	SBB	38163574238	Serbia	
Jump6times	Jump Tmes	Ivanka.b.Milosevic	178.149.75.60	SBB	38163574238	Serbia	
Lazypandamail	Lazy panda	siera@sbb.rs	178.149.197.6	SBB			
m.jovana.joka98	Jovana Milosevic	siera@sbb.rs	188.2.134.18	SBB Modem			
Madonna.picture.sell	Siera Smith	siera@sbb.rs	188.2.141.193	SBB Modem	38163574238	Serbia	
Mmaria244562	Maria Magdalena		188.2.13.156	SBB Modem	38163574238	Serbia	
Nameless244562	Nameless nameless	siera@sbb.rs	178.149.72.177 109.202.157.136	SBB Norway	38163574238	Serbia	

Appendix B

Frhtlayout Email Account Summary

Address	Name	Recovery Email	IPs	SMS	SMS Country	Cookies
Frhtlayout (Original Frhylaout Account)	**P Domingues**	**myfavouritenightmare**	**177.81.142.224 201.93.22.71 189.46.62.229 177.79.41.54 177.102.114.248 189.0.82.161 191.254.165.252**	**5511998560016**	**Brazil**	**MyfavouriteNightmare Paloma.discola@usp.br**
Daichi.bloodlust	Daichi	myfavouritenightmare	177.81.94.43	5511998560016	Brazil	
dmngsp	Paloma Domingues	myfavouritenightmare	179.208.63.123	5511998560016	Brazil	
izildadomingues	Izilda Domingues	myfavouritenightmare	189.62.251.68 177.102.115.248 189.0.82.161	5511998560016	Brazil	
myfavoritenightmare	Paloma Domingues	Domingues.p@outlook.com	200.207.5.180 201.93.22.71 189.46.62.229 177.102.114.248	5511998560016	Brazil	
Paloma.discola@usp.br	Paloma Discola Domingues Silva	Paloma.discola@usp.br.test	201.93.22.71 189.46.62.229 177.102.115.248 191.254.165.252		Brazil	

[i] Not all IP addresses are listed for each account

ATTACHMENT A

Google Accounts to be Searched

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data associated with the following Google accounts (collectively, the "Subject Accounts"), that are stored at premises controlled by Google, a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California:

a. im244562@gmail.com;
b. im514238@gmail.com;
c. 244562im@gmail.com;
d. blekpendaz@gmail.com;
e. carpetcleanerexpert8@gmail.com;
f. celebrityfascination@gmail.com;
g. hexenbiest316@gmail.com;
h. hqphotosworld@gmail.com;
i. im250372@gmail.com;
j. im308009@gmail.com;
k. imilosevic514@gmail.com;
l. ivanka.b.milosevic@gmail.com;
m. jovna.milosevic@gmail.com;
n. joximilosevic@gmail.com;
o. Jump2times@gmail.com;
p. Jump6times@gmail.com;
q. lazypandamail@gmail.com;
r. m.jovana.joka98@gmail.com;
s. madonna.picture.sell@gmail.com;
t. Mmaria244562@gmail.com; and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

u. nameless244562@gmail.com.

v. frhtlayout@gmail.com;

w. myfavouritenightmare@gmail.com;

x. daichi.bloodlust@gmail.com;

y. dmngsp@gmail.com;

z. izildaddomingues@gmail.com; and

aa. paloma.discola@usp.br.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

I. Information to be disclosed by Google, for search:

1. To the extent that the information described in Attachment A is within the possession, custody, or control of Google, including any e-mails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google, is required to disclose the following information to the government for each of the Subject Accounts listed in Attachment A:

a. All electronic mail content and/or preserved data (including e-mail, attachments, and embedded files);

b. All subscriber records associated with the specified account, including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by Google in relation to the account; 6) account log files (login IP address, account activation IP address, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;

c. all contact lists;

d. all Google Calendar content;

e. all Google Drive content;

f. all Google Sheets content;

g. all Google Forms content;

h. all Google Apps Script content;

i. all Google Maps content;

j. all Google Photos content;

k. all Google Search Console content;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

l. all Google Web & Activity content;

m. all Google Chrome Sync content;

n. all Google Location History content;

o. all Google Developers Console content;

p. all Google Voice content;

q. all Android content;

r. all Google Alerts content;

s. all Google Profile content;

t. all account history, including any records of communications between Google and any other person about issues relating to the accounts, such as technical problems, billing inquiries, or complaints from other users about the specified account. This is to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber in connection with the service.

II. Information to be seized by the government

All information that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18, United States Code, Sections 1029 (Access Device Fraud), 1030(a)(4) (Computer Fraud), 1343 (Wire Fraud), 1028A (Aggravated Identity Theft), 1349 (Conspiracy to Commit Wire Fraud), and 371 (Conspiracy), for each account or identifier listed on Attachment A, including the following:

a. Content that serves to identify any person who uses or accesses the subject accounts or who exercises in any way any dominion or control over the accounts;

b. Content relating to planned, attempted, or successful breaches of or intrusions into victims' computers or networks;

c. Content relating to the purchase, sale, offer for purchase or sale, acquisition, or transfer of credentials that can be used to access digital content;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

d. Any material referencing the AfterEF forum or any member of the AfterEF forum;

e. Content that may identify victims of computer intrusions perpetrated by the account holders;

f. Content that may constitute communications in furtherance of the crimes enumerated above;

g. Content that may identify assets including bank accounts, commodities accounts, trading accounts, personal property and/or real estate that may represent proceeds of intrusion activity or fraud or are traceable to such proceeds;

h. Content that may reveal the current or past location of the individual or individuals using the subject accounts;

i. Content that may reveal the identities of and relationships between co-conspirators;

j. Content that may identify any alias names, online user names, "handles" and/or "nics" of those who exercise in any way any dominion or control over the specified accounts as well as records or information that may reveal the true identities of these individuals;

k. Other log records, including IP address captures, associated with the specified account;

l. Records or information showing the location from which the account user has accessed or utilized the accounts, including GPS, Wi-Fi, or cell tower proximity records related to the accounts;

m. Address lists or buddy/contact lists associated with the subject accounts;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

n. Subscriber records associated with the specified accounts, including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by Google in relation to the accounts; 6) account log files (login IP address, account activation IP addresses, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;

o. Records of communications between Google and any person purporting to be the account holder about issues relating to the accounts, such as technical problems, billing inquiries, or complaints from other users about the specified account. This is to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications; and

p. Information identifying accounts that are linked or associated with the subject accounts.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Google, Inc., and my official title is _____. I am a custodian of records for Google, Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google, Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Google; and

c. such records were made by Google, Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____ _____

Date Signature

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970